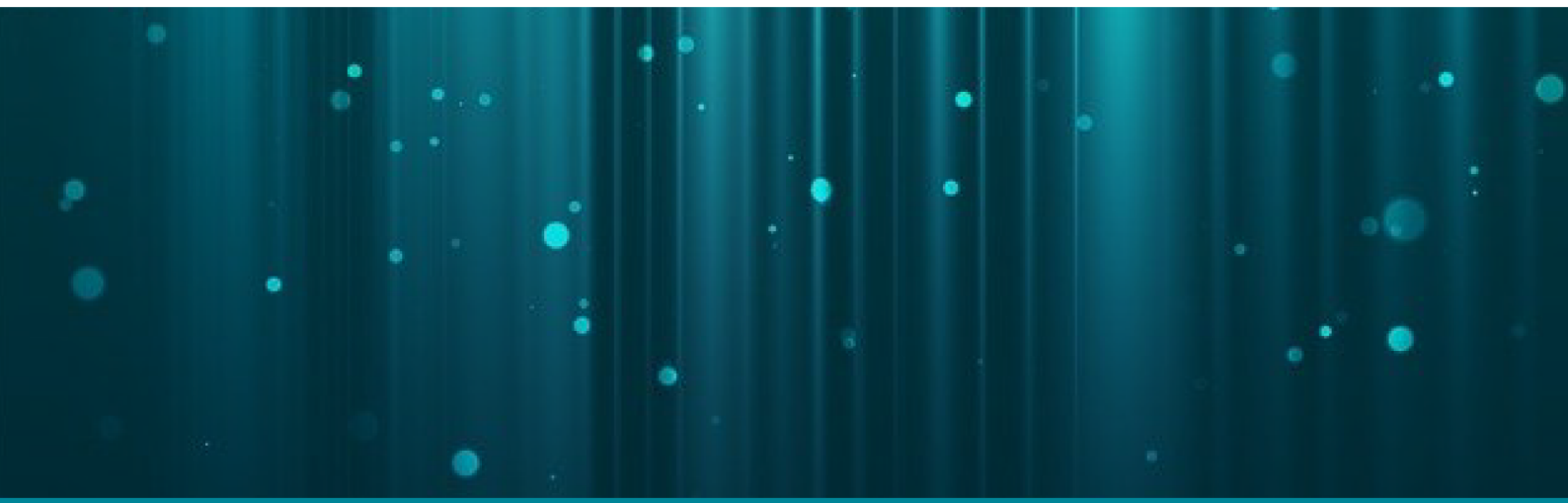
OneSpan



DIGIPASS FX1 BIO

User Manual

Version: 2023-10-05

Copyright Notice

Trademarks

Intellectual Property

Disclaimer

OneSpan accepts no liability for the accuracy, completeness, or timeliness of content, or for the reliability of links to and content of external or third party websites.

OneSpan shall have no liability under any circumstances for any loss, damage, or expense incurred by you, your company, or any third party arising from the use or inability to use OneSpan Software or Materials, or any third party material made available or downloadable. OneSpan will not be liable in relation to any loss/damage caused by modification of these Legal Notices or content.

Reservation

OneSpan reserves the right to modify these Notices and the content at any time. OneSpan likewise reserves the right to withdraw or revoke consent or otherwise prohibit use of the OneSpan Software or Materials if such use does not conform to the terms of any written agreement between OneSpan and you, or other applicable terms that OneSpan publishes from time to time.

Contact us

Visit our website: **https://www.onespan.com**
Resource center: **https://www.onespan.com/resource-center**
Technical support and knowledge base: **https://www.onespan.com/support**

If there is no solution in the knowledge base, contact the company that supplied you with the OneSpan product.

Date: 2023-10-05

Contents

Figures

Tables

Procedures

Product overview

1

Welcome to the *DIGIPASS FX1 BIO User Manual*! DIGIPASS FX1 BIO is a phishing-resistant authenticator that works out-of-the-box with hundreds of FIDO2–enabled services.

The **FIDO Alliance** develops standards for passwordless authentication. With FIDO (Fast IDentity Online), user authentication does not rely on static passwords or one-time passwords. Instead, users are authenticated via biometrics and FIDO–compliant authenticators.

The DIGIPASS FX1 BIO authenticator works in connected mode via USB, Bluetooth LE (BLE), or NFC.

1.1 Device overview

1.1.1 Authenticator front

Figure 1: Authenticator front

1 Power button/Bluetooth pairing mode button

2 Foldable USB-C cable

3 LED indicators

4 Fingerprint sensor

1.1.2 Authenticator back

Regulatory identifiers are printed on the back of the authenticator.

Figure 2: Authenticator back

1.1.3 USB cable manipulation

The USB cable can be folded at the back of the authenticator, thanks to a magnetic mechanism. You do not need a separate USB cable for USB-connected operations.

Figure 3: USB-C cable

To unclip the USB cable, lift the metallic part of the USB plug to release the magnet (**1**), or pull the cable at the tip of the plastic cap (**2**).

> **CAUTION:** To ensure maximum longevity, do not twist or fold the cable at sharp angles, since this can damage the cable.
>
> Do not hold the authenticator's main body to pull the USB cable. Pull the authenticator by holding the plastic plug.

1.2 PIN protection

The DIGIPASS FX1 BIO authenticator performs user verification primarily by fingerprint, and by PIN as a fall-back method.

Since the DIGIPASS FX1 BIO authenticator has no keypad, the PIN is entered on the device to which the authenticator is connected (typically a PC or a smartphone).

The PIN is composed of alphanumeric characters and must comply with the following rules:

- **Minimum length**: 4 decimal digits or 4 characters
- **Maximum length**: 63 bytes in UTF-8 representation. This corresponds to 63 characters if only standard ASCII characters are used, but corresponds to fewer characters if special characters are used (e.g. accented, Chinese,...).

NOTE: After 3 consecutive incorrect PIN attempts, the authenticator must be turned off and restarted before a new PIN attempt can be made. In case of a USB connection, this is done by removing and re-inserting the USB cable. In case of BLE or NFC communication, this is done by either explicitly turning off the authenticator with the Power button, or letting the device turn off automatically via time-out, and then turning it on again.

CAUTION: After a total of 8 consecutive incorrect PIN attempts, the authenticator is locked. The authenticator must be reset, which effectively removes all data (credentials, accounts, fingerprint, PIN) and reverts the authenticator to factory settings.

1.3 Fingerprint sensor

The fingerprint sensor is used to verify the user. The sensor is a 360° sensor and recognizes a fingerprint in any orientation. There are two verification modes:

- **Touch only.** In this mode, the fingerprint LED blinks BLUE ● ● ●. Any finger can be used. This mode confirms **the user's presence, but not their identity**.

> **NOTE:** In case of an NFC connection, the method for confirming the user presence can vary depending on the relevant service. You may need to tap the authenticator against the NFC reader field, or touch the fingerprint.

- **Verification.** In this mode, the fingerprint LED blinks MAGENTA ● ● ●. This mode is used to **verify the user** if at least one fingerprint is enrolled. You need to use a fingerprint that has been enrolled.

> **CAUTION:** After 5 consecutive unsuccessful fingerprint attempts without any correct PIN entry in between, fingerprint verification is disabled until a correct PIN is entered. While the fingerprint verification is disabled, the PIN must be entered instead, followed by a finger touch on the sensor (to verify user presence).
>
> A correct PIN entry resets both the PIN error counter and the fingerprint error counter. A correct fingerprint match resets only the fingerprint error counter, and not the PIN error counter.

1.3.1 Fingerprint enrollment

Fingerprint enrollment is the process of registering a fingerprint template, i.e. a mathematical image of a fingerprint, in the authenticator. With this, it is possible to identify the user by a simple finger touch on the fingerprint sensor. You need to configure the PIN before you can enroll a fingerprint. This is because the PIN serves as a fall-back method in case of unsuccessful fingerprint attempts.

The authenticator can save up to 5 fingerprint templates. If you try to enroll an additional fingerprint, the device returns an error message to indicate that no fingerprint enrollment can be performed. You can then free up space by removing one or several fingerprint templates. For information about deleting enrolled fingerprints, see **4.3.2 Delete enrolled fingerprints**.

NOTE: In the *Windows Settings app*, if you try to enroll a fingerprint and the fingerprint storage is already full, a general error message will be displayed, indicating that something went wrong during enrollment.

1.4 LED indicators

The device has three LEDs on its front side, which indicate the status of Bluetooth, fingerprint, and battery level.

Table 1: Description of Bluetooth LED

LED	Description
 Off	Bluetooth is disabled, or enabled but there is no connection, and pairing mode is not currently active.
● ● ● Blinking BLUE	Bluetooth pairing mode.
● BLUE	Connected to a Bluetooth host.

Table 2: Description of fingerprint LED

LED	Description
 Off	Idle state.
● ● ● Blinking BLUE	Waiting for finger touch for user presence detection. Any finger can be used.
● ● ● Blinking MAGENTA	Waiting for finger touch for user verification. An enrolled finger must be used. -OR- Waiting for finger touch during fingerprint enrollment.
● MAGENTA	Finger on the sensor, only for user verification.
● GREEN	Fingerprint match successful for user verification. -OR- Fingerprint image captured during enrollment.
●●●●● Fast blinking RED 5 times	Fingerprint match failed for user verification.
● YELLOW	Fingerprint image rejected because mobility is too low or coverage is too low, during enrollment. You are requested to slightly move/shift your finger and try again.

Table 3: Description of battery LED

LED	Description
 Off	Authenticator is turned off.

Table 3: Description of battery LED (continued)

LED	Description
🔴🔴🔴🔴🔴 Fast blinking RED 5 times then power off	Battery at critical level, USB not connected.
🟡 🟡 🟡 Blinking ORANGE	Battery at warning level or lower, USB not connected.
🟢 🟢 🟢 Blinking GREEN	Battery charging, USB connected.
🟢 GREEN	Battery fully charged, USB connected. -OR- Battery at normal level, USB not connected.
🟣🟣🟣🟣🟣 Fast blinking MAGENTA	Battery charging disabled because out of operational temperature range (under 0°C or above 45°C).

1.5 Charge the battery

To recharge the authenticator, plug the USB cable into the USB port of a PC, phone, or wall charger. Once the battery is fully charged, the battery LED indicator stops blinking and turns GREEN ●.

> **NOTE:** As a safety measure, battery charging is disabled if the device is out of its operational temperature range (0°C–45°C). On the authenticator, this protection is visualized by a fast blinking of the battery LED in MAGENTA ●●●●●.

Getting started

2

2.1 First steps

2.1.1 Turn the authenticator on/off

In standalone mode (without USB connection)

- To turn on the authenticator, press the Power button for one second.
- To turn off the authenticator, press and hold the Power button.
- The authenticator will automatically turn off after 60 seconds of inactivity.

In USB-connected mode

- To turn on the authenticator, plug the USB cable.
- To turn off the authenticator, unplug the USB cable.

> **NOTE:** When you use the DIGIPASS FX1 BIO authenticator for the first time, you need to connect the authenticator via USB. You will not be able to turn it on by pressing the Power button.

2.1.2 Connect your authenticator

You can connect your authenticator via Bluetooth LE, USB, or NFC.

2.2 Initial authenticator setup

The following applications provide facilities to set up and manage your authenticator:

- On *Windows*, you can manage your authenticator in the Windows Settings app.
- On *macOS* and *Linux*, you can manage your authenticator via the Google Chrome security settings.

The initial authenticator setup involves the following steps:

1. Set the PIN
2. Enroll a fingerprint

> **NOTE:** You need to set the PIN before you can enroll a fingerprint.

2.2.1 Windows

▸ To set the PIN (Windows Settings app)

1. Connect your authenticator.
2. Click the Start button on your computer and select **Settings** to open the Windows Settings app.
3. Select **Accounts > Sign-in options**.
4. Click **Security Key**, then click **Manage**.
5. When prompted, touch the fingerprint sensor on the authenticator.

   The **Windows Hello setup** dialog is displayed.
6. Under **Security Key PIN**, click **Add**.
7. Specify and confirm the authenticator PIN, and click **OK**. See **1.2 PIN protection** for PIN requirements.

▸ To enroll a fingerprint (Windows Settings app)

1. In the **Windows Hello setup** dialog, under **Security Key Fingerprint**, click **Set up**.
2. Enter your PIN and click **OK**.
3. Follow the on-screen instructions to enroll your fingerprint.
4. When fingerprint enrollment is completed, click **Done**.

2.2.2 macOS and Linux

▸ To set the PIN (Google Chrome)

1. Connect your authenticator.
2. In Google Chrome, navigate to the **Manage security keys** page:
   - Click ⋮ **Customize and control Google Chrome** and select **Settings > Privacy and security > Security > Manage security keys**.

   -OR-

   - Type the following address in the address bar: chrome://-settings/securityKeys
3. Click **Create a PIN**.
4. When prompted, touch the fingerprint sensor on the authenticator.
5. Specify and confirm the PIN, and click **Save**. See **1.2 PIN protection** for PIN requirements.
6. Click **OK** to complete the PIN creation.

▸ To enroll a fingerprint (Google Chrome)

1. On the **Manage security keys** page, click **Fingerprints**.
2. When prompted, touch the fingerprint sensor on the authenticator.
3. Enter the PIN and click **Continue**.

4. In the **Manage fingerprints** dialog, click **Add**.
5. Follow the on-screen instructions to enroll your fingerprint.
6. When the fingerprint has been captured, click **Continue**.
7. Specify a name for the fingerprint and click **Continue**.
8. Click **Done** to complete the fingerprint enrollment.

2.3 Use the authenticator

The steps for using the DIGIPASS FX1 BIO authenticator vary depending on your application provider's setup. See **3 FIDO authentication** for an overview of the FIDO registration and sign-in process.

FIDO authentication

3

For FIDO authentication, you first need to register your DIGIPASS FX1 BIO authenticator with the relevant service. After successful registration, you can sign in to the service with your fingerprint.

> **NOTE:** FIDO operations are accessible via compatible browsers.

3.1 Get started with FIDO authentication

Registration and authentication workflows vary depending on the options that are used by the browser and the platform.

3.1.1 Before you begin

Before you can get started with FIDO authentication, ensure that you have completed the initial authenticator setup. For more information, see **2.2 Initial authenticator setup**

3.1.2 Register the authenticator and sign in

▸ To register the authenticator

1. Connect your authenticator via USB, Bluetooth LE, or NFC.
2. Follow the instructions for the relevant service to register the authenticator for FIDO authentication.

   During the registration process, you usually need to name the authenticator, and provide your fingerprint and/or your PIN.

> **NOTE:** The DIGIPASS FX1 BIO authenticator can save up to 100 discoverable credentials.

▸ To sign in using FIDO authentication

1. Connect your authenticator via USB, Bluetooth LE, or NFC.
2. Follow the instructions for the service to which you want to sign in.

   When prompted, provide your fingerprint and/or PIN for authentication.

Manage the authenticator

4

Depending on your operating system, you can use the following applications for authenticator management:

- On *Windows*, you can manage your authenticator in the Windows Settings app.
- On *macOS* and *Linux*, you can manage your authenticator via the Google Chrome security settings.

4.1 Manage Bluetooth settings

Before you can connect your DIGIPASS FX1 BIO authenticator over Bluetooth LE, you need to pair it with the host device.

4.1.1 Before you begin

Windows 11

If you are using Windows 11, you need to enable *advanced Bluetooth devices discovery* to be able to pair the authenticator.

▸ To enable advanced Bluetooth devices discovery

1. Click the Start button on your computer and select **Settings** to open the Windows Settings app.
2. Select **Bluetooth & devices > Devices**.
3. In the **Device settings** section, select **Advanced** for **Bluetooth devices discovery**.

4.1.2 Pair a new device

▸ To pair a new device

1. To activate the pairing mode, press and hold the Power button for a minimum duration of 5 seconds. While the authenticator is in pairing mode, the Bluetooth LED is blinking BLUE ●●●.

   In pairing mode, the authenticator is visible by any nearby device over Bluetooth, under the name “DIGIPASS FX1 BIO”.
2. Follow the instructions on your host device to add a new Bluetooth device.
3. Once the DIGIPASS FX1 BIO authenticator is detected on the host device, enter the pairing code 000000 (6 times zero) on the host device to complete the pairing process.

NOTE: After successful pairing, the authenticator will automatically disconnect. It will re-connect only when you perform FIDO operations (FIDO registration and authentication, fingerprint enrollment, etc.).

The DIGIPASS FX1 BIO authenticator can store a maximum of 4 paired devices. If the maximum is reached and a new device is paired, it replaces the oldest one that is stored.

4.2 Change the PIN

4.2.1 Windows

▸ To change the PIN (Windows Settings app)

1. Connect your authenticator and open the **Windows Hello setup** dialog in the Windows Settings app. See **2.2 Initial authenticator setup** for instructions to open the dialog.
2. Under **Security Key PIN**, click **Change**.
3. Do the following:
   a. Enter the old PIN.
   b. Enter and confirm the new PIN.

   See **1.2 PIN protection** for PIN requirements.
4. Click **OK**.

4.2.2 macOS and Linux

▸ To change the PIN (Google Chrome)

1. Connect your authenticator.
2. On the **Manage security keys** page of the Google Chrome security settings, click **Create a PIN**. See **2.2 Initial authenticator setup** for instructions to open the page.
3. When prompted, touch the fingerprint sensor on the authenticator.

4. Do the following:
    a. Enter the old PIN.
    b. Enter and confirm the new PIN.

    See **1.2 PIN protection** for PIN requirements.
5. Click **Save**.

4.3 Manage fingerprints

4.3.1 Enroll additional fingerprints

Windows

▸ To enroll an additional fingerprint (Windows Settings app)

1. Connect your authenticator and open the **Windows Hello setup** dialog in the Windows Settings app. See **2.2 Initial authenticator setup** for instructions to open the dialog.
2. Under **Security Key Fingerprint**, click **Add another**.
3. Enter your PIN and click **OK**.
4. Follow the on-screen instructions to enroll your fingerprint.

> **NOTE:** If the fingerprint image is too similar to a previous one, the sensor cannot get enough data to build the template. In this case, the fingerprint LED will turn YELLOW ● and you need to slightly change the angle and/or position of your fingertip on the sensor.

5. When the fingerprint enrollment is completed, click **Done**.

macOS and Linux

▸ To enroll an additional fingerprint (Google Chrome)

1. Connect your authenticator.
2. On the **Manage security keys** page of the Google Chrome security settings, click **Fingerprints**. See **2.2 Initial authenticator setup** for instructions to open the page.
3. When prompted, touch the fingerprint sensor on the authenticator.
4. Enter the PIN and click **Continue**.

5. In the **Manage fingerprints** dialog, click **Add**.
6. Follow the on-screen instructions to enroll your fingerprint.

> **NOTE:** If the fingerprint image is too similar to a previous one, the sensor cannot get enough data to build the template. In this case, the fingerprint LED will turn YELLOW ● and you need to slightly change the angle and/or position of your fingertip on the sensor.

7. When the fingerprint has been captured, click **Continue**.
8. Specify a name for the fingerprint and click **Continue**.
9. Click **Done** to complete the fingerprint enrollment.

4.3.2 Delete enrolled fingerprints

Windows

In Windows, it is not possible to remove individual fingerprints. If you want to delete a fingerprint, you need to delete all enrolled fingerprints.

▸ To delete all fingerprint templates (Windows Settings app)

1. Connect your authenticator and open the **Windows Hello setup** dialog in the Windows Settings app. See **2.2 Initial authenticator setup** for instructions to open the dialog.
2. Under **Security Key Fingerprint**, click **Remove**.
3. Enter your PIN and click **OK**.

   All fingerprints that are stored on the authenticator are deleted.

macOS and Linux

In Google Chrome, you can view the list of enrolled fingerprints. From this list, you can select the fingerprint that you want to remove.

▸ To delete a fingerprint template (Google Chrome)

1. On the **Manage security keys** page of the Google Chrome security settings, click **Fingerprints**. See **2.2 Initial authenticator setup** for instructions to open the page.
2. When prompted, touch the fingerprint sensor on the authenticator.
3. Enter the PIN and click **Continue**.
4. In the **Manage fingerprints** dialog, locate the relevant fingerprint and click **x Delete**.
5. Click **Done**.

4.4 Remove FIDO credentials

4.4.1 Windows

The Windows Settings app does not support the removal of FIDO credentials.

4.4.2 macOS and Linux

In Google Chrome, you can view the list of discoverable credentials, and delete credentials as needed.

▸ To remove FIDO credentials (Google Chrome)

1. Connect your authenticator.
2. In the **Manage security keys** page of the Google Chrome security settings, click **Sign-in data**. See **2.2 Initial authenticator setup** for instructions to open the page.
3. Locate the relevant credentials in the list and click the **Delete** icon.
4. Click **Done**.

4.5 Reset authenticator

In some situations it is necessary to restore the factory settings of the DIGIPASS FX1 BIO authenticator, for example if the PIN is locked.

A factory reset deletes all personal information that is stored on the authenticator:

- PIN
- All fingerprint templates
- All credentials
- All accounts
- All Bluetooth pairings

> **NOTE:** Resetting the authenticator is possible only via a USB connection. You *cannot* reset the authenticator via BLE or NFC connections.

4.5.1 Windows

▸ To reset the authenticator (Windows Settings app)

1. Connect your authenticator and open the **Windows Hello setup** dialog in the Windows Settings app. See **2.2 Initial authenticator setup** for instructions to open the dialog.
2. Under **Reset Security Key**, click **Reset**.
3. Click **Proceed** to confirm that you want to reset the authenticator.
4. When prompted, disconnect and reconnect the authenticator.
5. When prompted, touch the fingerprint sensor on the authenticator twice within 10 seconds after you have reconnected the authenticator.
6. When the reset is completed, click **Done**.

4.5.2 macOS and Linux

- To reset the authenticator (Google Chrome)

1. Connect your authenticator.
2. On the **Manage security keys** page of the Google Chrome security settings, click **Reset your security key**. See **2.2 Initial authenticator setup** for instructions to open the page.
3. When prompted, disconnect and reconnect the authenticator, then touch the fingerprint sensor on the authenticator.
4. When prompted, touch the fingerprint sensor on the authenticator to confirm the factory reset.
5. Click **OK** to complete the factory reset.

Technical specifications and system requirements

5

5.1 Technical specifications

Table 4: Technical specifications for DIGIPASS FX1 BIO

Size	35mm (49.5 w/cable) (L) x 35(W) x 10.8mm(H)
Weight	11g
Fingerprint sensor	Capacitive
Bluetooth	Bluetooth 5.2 LE (Low Energy)
NFC	ISO 14443 / card-emulation mode / extended APDU support
Battery	Rechargeable - 65 mAh
Cable	Integrated USB-C cable
Power supply in connected mode	Via USB-C, 4.75 to 5.50 volts
Dust & water resistance	Dust-safe and splashproof
Supported protocols	FIDO: • FIDO U2F • FIDO2.1: the device implements the CTAP2.1 specification

5.1.1 Battery performance

To optimize the performance of the rechargeable battery, use and charge your DIGIPASS FX1 BIO authenticator at least once every two months.

5.2 System requirements

Supported operating systems:

- Windows 10 version 1903 or later
- macOS 13 or later
- Ubuntu 22.04.2 or later
- Android 12 or later

Supported browsers:

- Google Chrome 111 or later
- All browsers that support the *FIDO2 WebAuthn API*

> **NOTE:** For a list of compatible operating systems and browsers, refer to **https://www.onespan.com/digipassfidofx1bio**.

Safety notice and regulatory information

6

6.1 Safety notice

CAUTION: Failure to observe the safety instructions can result in fire, electric shock and other injuries or damage to the device or other property. The housing is made of plastic with sensitive electronic components and batteries inside.

Safety instructions

- Do not pierce, break, crush, or cut the device or the battery.
- Do not expose the device or the battery to an open flame or extremely high temperatures.
- Do not expose the device or the battery to liquids or extremely low air pressure.
- Do not drop the device or the battery.
- The device or the battery must be recycled or disposed of separately from household waste.

6.2 Regulatory and compliance information

Table 5: Certification and compliance

Short-term storage temperature	• -10° C to 50° C • 90% RH non-condensing	• IEC60068-2-78 (damp heat) • IEC60068-2-1 (cold)
Operating temperature	• 0° C to 45° C • 85% RH non-condensing	• IEC60068-2-78 (damp heat) • IEC60068-2-1 (cold)
Vibration	• 10 to 75 Hz • 10 m/s^2	• IEC60068-2-6
Drop	• 1 meter	• IEC60068-2-31
Emission		• EN55022
Immunity	• 4 kV contact discharges • 8 kV air discharges • 3 V/m from 80 to 1000 MHz	• EN55024
Compliant with European Directives	• CE: 89/336/EEC or 2004/108/EC • RoHS: 2002/95/EC • WEEE: 2002/96/EC	
Compliant with Federal Communications Commission	• FCC ID: 2AH88-FX1B • IC: 27700-FX1B	

Statement of Compliance with EU Directive

CE OneSpan NV declares that this DIGIPASS FX1 BIO device is in compliance with the Essential requirements and other relevant provisions of Directive 2014/53/EU and 2015/863/EU.

The full Declaration of Conformity can be requested from:

Company: OneSpan NV

Address: Romeinsesteenweg 564C, 1853 Strombeek-Bever, Belgium

Email: legal@onespan.com

FCC Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications made to this equipment not expressly approved by OneSpan NV may void the FCC authorization to operate this equipment.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This portable transmitter with its antenna has shown compliance with FCC's SAR limits for general population / uncontrolled exposure. The antenna used for this device must not be co-located or operating in conjunction with any other antenna or transmitter.

IC Notice for Canada

This Class B device complies with Canadian ICES-003 requirements for Information Technology Equipment (including Digital Apparatus). Cet appareil numerique de la classe B est conforme a la norme NMB-003 du Canada.

This Device complies with Industry Canada License-exempt RSS standard(s). Operation is subject to the following two conditions: 1) this device may not cause interference, and 2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: 1) l'appareil ne doit pas produire de brouillage; 2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Correct disposal of this product (Waste Electrical and Electronic Equipment)

Applicable in the European Union and other European countries with separate collection systems

This marking shown on the product or its literature, indicates that it should not be disposed with other household waste at the end of its working life. To prevent possible harm to the environment or human health from uncontrolled waste disposal, please separate this from other types of waste and recycle it responsibly to promote the sustainable reuse of material resources. Household users should contact either the provider of the product, or their local government office, for details of where and how they can take this item for environmentally safe recycling. Business users should contact their supplier and check the terms and conditions of the purchase contract. This product should not be mixed with other commercial waste for disposal.